

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

ENTESAR OSMAN KASHEF, *et al.*,

Plaintiffs,

v.

BNP PARIBAS S.A., and BNP PARIBAS US
WHOLESALE HOLDINGS, CORP.,

Defendants.

No. 1:16-cv-03228-AKH

Hon. Alvin K. Hellerstein

**~~PROPOSED~~ PROTECTIVE ORDER GRANTING PLAINTIFFS' MOTION TO
COMPEL AND GOVERNING PRODUCTION AND USE OF PRODUCED DATA**

Upon consideration of Plaintiffs' Motion to Compel Compliance with Subpoenas *duces tecum* (ECF No. 564, the "Motion"), **IT IS HEREBY ORDERED** that the Motion is **GRANTED in part** and that the United States Department of Homeland Security (herein, "the Government") is compelled to produce the last known names, addresses, and contact information, if available, of potential class members, as maintained electronically in the ordinary course of business in the United States Citizen and Immigration Services' Central Index System.

Production shall be made in compliance with the following terms and specifications.

IT IS ORDERED THAT:

I. Production of Government Data.

1. **Identification of the Government Data and Production.** The Government shall produce the last known names, addresses, and contact information, if available, of potential class members, individuals who have ever been or currently are asylees and refugees in the United States, available in the United States Citizen and Immigration Services' Central Index System (the "CIS 2 database"). The Government will identify potential class members by country of birth or

country of citizenship of Sudan, who entered the United States after November 4, 1997, and who had a class of admission (“COA”) in their case history of Refugee or Asylee, or associated COAs.

2. The Government shall only produce last known names, addresses, and contact information, if available, of potential class members (the “Government Data”), as maintained in the ordinary course of business in the CIS 2 database. The Government Data is to be produced in an encrypted native Excel file format, with the following columns separated out where possible¹:

- (i) Last Name;
- (ii) Middle Name;
- (iii) First Name;
- (iv) Address Number and Street Name;
- (v) Apartment Number;
- (vi) City;
- (vii) State;
- (viii) Zip Code;
- (ix) Phone number;
- (x) Email address.

3. **Production Recipient.** The Government Data shall only be produced to Epiq Class Action and Claims Solutions, Inc. (“Epiq” or the “Recipient”), the court-appointed notice administrator,² courtesy of Stephen Donaldson, Program Director (stephen.donaldson@epiqglobal.com). The Government Data shall also be provided *ex parte* under seal to the Court and shall be accessible only by the Court and Epiq, but not the parties. The

¹ The Government will provide all data points requested if available in the CIS 2 database. Where a column for a field is empty in the Excel file, the Recipient should assume that the Government does not have the data to share.

² In a contemporaneous order, Epiq is named as the class notice administrator in this litigation.

Government Data shall not be produced to Plaintiffs or Defendants in this litigation, unless ordered otherwise by the Court.

4. **Production date and format.** The Government Data shall be produced to the Recipient by December 6, 2024, via a secure encrypted electronic file transfer or file sharing system (*e.g.*, Secure File Transfer Protocol (SFTP site), Encrypted email, etc.).

5. **Limitations:** Nothing in this Order shall be interpreted to require disclosure of any other data contained in the CIS 2 database or any other database or source available to the Government.

II. **Protective Order.**

6. **Protected Material.** The Government Data, at a minimum as it relates to refugees and asylees, is protected Highly Confidential material. The obligations imposed herein shall remain in effect until and unless the Court orders otherwise.

7. **Access to and Use of the Government Data.** Unless otherwise ordered by the Court or permitted in writing by the Government, the Recipient must protect the confidentiality of the Government Data, and may not disclose or use the Government Data, or a subpart of the Government Data, for any purpose whatsoever, except as provided below, and only as necessary for the Recipient's work as appointed notice administrator in this litigation, as described in the accompanying Supplemental Declaration of Cameron R. Azari Regarding Noticing and Potential Class Member Data dated November 12, 2024:

- (i) To effectuate direct notice to potential class members by mail, by email, or by text message, as approved, ordered, and supervised by the Court;
- (ii) To update or verify the Government Data using sophisticated tools and third-party services, in compliance with industry standards and strict privacy protections;

- (iii) To anonymize the data and create heat maps from this data for purposes of identifying geographic areas where potential class members are localized, for purposes of notice; and
 - (iv) To anonymize the data and create general statistics and reports, to inform both the Court and the parties during the pendency of the notice process.
8. At Epiq, the Government Data may only be accessed by the following individuals:
- (i) **Stephen Donaldson**, Program Director ;
 - (ii) **Amanda Sternberg**, Director, Client Services Programs ;
 - (iii) **Jonathan Edwards**, Client Services Project Manager;
 - (iv) **Stephen Walker**, Client Services Associate Project Manager ;
 - (v) **Jackie Womack**, Client Services Associate Project Manager;
 - (vi) A limited number of required IT professionals, who have separate Windows Authentication credentials, logging, and monitoring than database users and who do not access individual data records but rather manage and monitor the environment, including server hardware, infrastructure, and licensing;
 - (vii) Any other person to whom the Government agrees in writing, or any other person to whom the Court orders access.

9. The individuals listed in Paragraph 8 above (each a “Receiving Individual”) must have read a copy of this Order and have signed the “Agreement to be Bound” attached as Exhibit A hereto before receiving access to the Government Data. Copies of each such signed Agreement to be Bound shall be maintained by Epiq for one year following the final termination of this litigation, including any appeals, and shall be made available to the Court or the Government if requested.

10. The Government Data must be stored and maintained by the Recipient in a secure and safe manner that ensures that access is limited only to the persons authorized under this Order. The Recipient will use the centrally-managed antivirus software, Microsoft Defender, across the organization providing real time blocking and alerting, and adhere to stringent standards for security expected for protecting highly confidential data in the industry. The Recipient shall

exercise at least the same standard of due and proper care with respect to the storage, custody, use, and/or dissemination of the Government Data as is exercised by the Recipient with respect to its own proprietary information.

11. If the Recipient discovers a breach of security, including any actual or suspected unauthorized access, relating to the Government Data, the Recipient shall: (1) promptly (i.e., within forty-eight hours of discovery) provide written notice by email and overnight delivery to the Government (c/o Assistant United States Attorney Jeffrey Oestericher, U.S. Attorney's Office for the Southern District of New York, 86 Chambers Street, 3rd Floor, New York, NY 10007; jeffrey.oestericher@usdoj.gov) and the Court of such breach; (2) immediately investigate and make prompt reasonable efforts to remediate the effects of the breach; (3) provide sufficient information about the breach that the Government and the Court can reasonably ascertain the size and scope of the breach; and (4) promptly take all necessary and appropriate steps to prevent a further breach. In any event, the Recipient shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access.

12. **Final Disposition.** After termination of the litigation, the provisions of this Order shall continue to be binding, except with respect to any information that becomes a matter of public record.

13. Unless otherwise ordered by the Court or agreed in writing by the Government, within thirty (30) days of the final termination of the litigation by dismissal, judgment, or settlement, including any appeals, the Recipient and each Receiving Individual must permanently destroy all of the Government Data in its possession. The Recipient must submit a written certification to the Government within five business days following the thirty-day deadline that avers under penalty of perjury that the Government Data was permanently destroyed and that the

Recipient and the Receiving Individuals have not retained any copies of or other forms of reproducing or capturing any of the Government Data.

14. **Violations of Order.** In the event that any person or entity should violate the terms of this Order, the Government may apply to the Court to obtain relief or the Court may grant relief *sua sponte*. This Court shall have jurisdiction over the Recipient and any other person or entity subject to the terms of this Order for enforcement of the provisions of this Order, including following the termination of the litigation.


III. Miscellaneous.

15. **Obligation to Meet and Confer.** Class Counsel and the Government shall meet and confer in an attempt to resolve any issues that arise in the implementation of this Order, prior to bringing the dispute to the Court unless exigent circumstances dictate otherwise.

16. **Modification:** This Order, and incorporated Exhibit A, may be modified by written agreement of Class Counsel and the Government, or by the Court.

IT IS SO ORDERED.

Dated: Nov. 18, 2024


Hon. Alvin K. Hellerstein
United States District Judge